REMARKS

Pending Claims

Claims 7, 9 - 11, 14 -17, 19, 22, 24, 26, 28 - 29 are pending. Claims 7, 9-11, 24, 26 and 28 have been amended. Claim 29 is presently introduced. No new matter has been added. Claims 21 and 27 have been cancelled without prejudice or disclaimer.

Claim Rejections Under 35 U.S.C. §102

Claims 7, 9-11, 14-17, 19, 21, 24 and 26 are rejected under 35 U.S.C. §102(e) as being anticipated by Martin, et al, U. S. Patent Publication No. 2003/0135783. Applicants request reconsideration of the rejection for the following reasons.

Applicants have amended claim 7, which is directed to a computer system including a host computer, storage system and storage control unit in combination with a data protection apparatus has been amended to include that the replication stopping unit instructs the storage control unit to stop the data replication from the first volume to the second volume when the event detection unit receives an event detection of an illegal intrusion into the host computer that is detected by an illegal intrusion detection unit. Claim 14 is also directed to a computer system including a host computer, storage system and storage control unit in combination with a data protection apparatus, also includes an event detection unit and a replication stopping unit for instructing the storage control unit to stop data replication from the first volume to the second volume when the event detection unit detects an event. In claim 14, the event detected by the event detection unit is a detection of a result of the differences between given data, with the detection result received from an alteration detection unit that reads the given data in a plurality of the second volumes to detect respective differences between the given data.

Claim 10 is directed to a data protection method for protecting data in a computer system and a data protection apparatus wherein the data protection method detects an intrusion into the host computer, instructs a storage unit to stop data replication from the first volume to the second volume when the intrusion is detected and stops the data replication in response to receiving the instruction. Claim 11 is directed to a program recorded on a computer readable medium that performs data protection in a computer system , that includes the detecting of an intrusion into a host computer and instructing the storage control unit to stop data replication from a first volume to a second volume when the intrusion is detected and stopping the data replication in response to receiving the instruction.

The method and system of the embodiments of the invention are for implementing data protection, for example, on a host computer, a storage system having at least one volume to store data, and a data protection apparatus. As shown in Fig. 7, the host computer 40, data protection apparatus 70, and storage system 60 are coupled to each other through a switch 50. The data protection apparatus includes an event detection unit, embodied as 73, for detecting the occurrence of events. The data protection apparatus also includes a replication stopping unit, embodied as 74, for instructing the storage control unit 63 controlling the volumes 64, 67a-67c located in the storage system 60.

Support for claims 7, 9-11, 14, 24 and 26 is provided with reference to Figures 6 and 7. In particular, the storage control unit 63 shown in Fig. 7 accepts an instruction from the replication stopping unit. The instruction stops data replication from storage area 64 to duplicate areas 67a-67c once the illegal intrusion unit or the alteration detection unit transmits an event detection to the event detection unit of the data protection apparatus 70.

The claimed embodiments of the invention are directed to data protection having a data protection apparatus which includes an event detection unit responsive to the occurrence of events on the host and a replication stopping unit responsive to the event detection unit. The replication stopping unit instructs the storage control unit to stop the replication of data stored on a first volume to a second volume storing data duplicated from the first volume. The replication stopping unit and step of stopping the replicating of data is further claimed to stop data replication when the event detection unit on the data protection apparatus receives an event detection from either an alteration detection unit or intrusion detection unit and instructs the storage control unit stop data replication. The replication stopping unit and step of stopping the replicating of data stops the replication of data from the first volume to the second volume, and as a result the claimed system and method of the invention provides that the data replicated to the second volume is secured when the replication is stopped to prevent potential damage to data stored on the second volume.

On the other hand, Martin discloses a primary storage device having a backup system including a replication driver 102 and a replicating controller 204. As shown in Figure 2 of Martin, the replicating controller of Martin is not comparable to the replication stopping unit claimed by applicants in claims 7 and 14 or to the step of stopping the data replication in claims 10 and 11. In Martin, the replication driver 102 provides a relay for requests to replicate data to a disk driver 104 and network driver 110. Likewise, the replicating controller 204 controls the primary storage 206 and replicates storage commands directed to the primary storage to the data management appliance 208. Martin uses replicated data stored on a data management appliance 114 to restore the data stored in primary storage 108, 206. Martin does not disclose preventing corruption or damage to data, but merely discloses restoring such corrupted or damaged data to a previous undamaged state.

The Office Action relies upon Figure 22 of Martin for disclosing a data management appliance 2204 that includes a virus scanner 2208. The virus scanner scans each individual virtual mirror for viruses. If a problem is located, the primary disk 2202 can be restored with the latest uninfected virtual mirror stored by data management appliance 2204. This is not equivalent to the intrusion detection unit, event detection unit or step of detecting an intrusion into the host computer that is claimed by applicants. In the claimed invention, the intrusion can be detected and then the replication of data from the first volume to the second volume is stopped in response to the detection of the event or the intrusion. This is not disclosed by Martin and therefore the rejection under 35 U.S.C. §102 of claims 7, 9-11, 14-17, 19, 21, 24, and 26 should be withdrawn.

Claim Rejections Under 35 U.S.C. §103

Claims 22-23 are rejected under 35 U.S.C. §103(a) as being unpatentable over Martin, et al '783 in view of Hickman et al, U. S. Patent Publication No. 2004/0236907. Claims 23, 25 and 27 have been canceled without prejudice or disclaimer. Applicants request reconsideration of the rejection of claims 22 and 28 for the following reasons.

Claims 22 and 28 both claim a path disconnection unit for instructing a storage control unit to stop communication between a host computer and storage system. The path disconnection unit instructs the storage control unit to stop when an event is detected by an event detection unit.

Martin is relied upon for disclosing the host computer (100, 200), storage system having first and second volumes (108, 114 and 206, 210) for storing data where the second volume is a duplicate of the first, a storage control unit (106, 202), and a data management appliance 2204 including a virus scanner 2208 and a replication driver and replicating controller 102, 204. However, Martin is silent with respect to disclosing a path disconnection unit for providing instruction to a storage control unit to stop communication between a host computer and storage system upon detection of an event by an event detection, as claimed by applicants.

Further, Hickman is relied upon for disclosing a path disconnection unit for stopping communication between a host computer and storage system, however Hickman is directed to the mirroring of storage devices for the purpose of updating code contained in a storage device and to allow a computer to boot from a second storage device while code is updated on a first storage device. Hickman fails to disclose implementing a path disconnection unit to stop communications between a host computer and a storage system in response to an event detection unit detecting an event, as claimed by applicants. Accordingly, the combination of Martin and Hickman does not render claims 22 and 28 unpatentable under 35 U.S.C. §103(a), and therefore the rejection should be withdrawn.

Conclusion

In view of the foregoing, Applicants respectfully request that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

Mattingly, Stanger, Malur & Brundidge, P.C.

By
John R. Mattingly
Reg. No. 30,293
(703) 684-1120

Date: June 23, 2008